

(FY 2013) PIA: System Information			
Program or System Name (as shown in SMART):		CDCO > AITC > VA > Purchase Care Program Integrity Tool	
OMB Unique System / Application / Program Identifier (AKA: UPID #):		029-00-01-11-01-5108-00	
Description of System/ Application/ Program : "must match what is stated in System Security Plan (SSP)" ***Do not type more than allotted space!!!***		<p>Purchase Care Program Integrity Tool (PIT), is part of Major Initiative (MI)-15 Health Care Efficiency. The PIT is comprised of multiple components. The data repository is at the core of the PIT system, it receives data feeds from other VA claim processing systems including Fee Basis Claims Systems (FBCS), Claims Processing and Eligibility (CP&E), and Corporate Data Warehouse (CDW); each source system providing data to a central drop zone.</p> <ol style="list-style-type: none"> 1. A central enterprise repository that will be fed from multiple claims systems to provide claims and patient clinical data through Extract Transform Load (ETL) Tools. 2. A Fraud/Waste/Abuse (FWA) or claims scoring application to detect and deter fraud/waste and abuse on pre-payment basis. 3. The dashboard and reporting application that accommodate end user browsing and analysis, standardized reports, ad hoc queries and reports and business intelligence extractions which we anticipate will be used to manipulate dimensional presentation of data. 4. A health care claims predictive modeling application principally used for FWA detection for the post-payment basis. <p>The foundation of the PIT model is a multidimensional schema consisting of dimension and fact entities. The PIT model consists of collections of star schemas aligned to multiple fact tables and conforming dimensions related to claim raw information and file alteration monitor (FAM) claims and provider scores.</p>	
Facility or Program Office Name:		Austin Information Technology Center (AITC)	
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
Information Security Officer:	Juan Rivera	732-578-5495	juan.rivera5@va.gov
System Owner/Delegate:	Tammy Watson	202-461-6126	tammy.watson@va.gov
Facility Chief Information Officer:*	N/A	N/A	N/A
Information Owner:			
Other Titles:			
Person Completing Document:	Eric Hutchinson	512-326-7876	eric.hutchinson@va.gov
Other Titles:			
Date of Last Full Approved PIA by VACO Privacy Services: (YYYY)			FY 2012
What specific legal authorities authorize this program or system:		Title 38, United States Code (U.S.C.), Sections 1710 and 1729	
What is the expected number of individuals that will have their PII stored in this system:			Approximately 2 million
Identify what stage the System / Application / Program is at:			Operations/Maintenance
The approximate date (MM/YYYY) the system will be operational (if in the Design or Development stage), or the approximate number of years the system/application/program has been in operation.			1 year
Is there an authorized change control process which documents any changes to existing applications or systems?			<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA
If No, (Explain on Tab 8)			
Is there a contingency plan in place to process information when the system is down?			<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA
Has a PIA been completed within the last three years?			<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> N/A : First PIA
FISMA QUESTIONS			
Answers provided in this section must correspond with the FISMA information listed in SMART for this system.			
1. Is this a new system?	<input type="radio"/> Yes <input checked="" type="radio"/> No		
2. Does this system contain Federal information in identifiable form?	<input checked="" type="radio"/> Yes <input type="radio"/> No		
3. Does the system include information on the public?	<input checked="" type="radio"/> Yes <input type="radio"/> No		
4. Is there a Privacy Impact Assessment (PIA) that covers this system?	<input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> National Security System under 40 U.S.C. 11103, a PIA is not required for this system		
5. Is Federal-owned information in this system retrieved by name or unique identifier?	<input checked="" type="radio"/> Yes <input type="radio"/> No		
6. What is the System of Records Notice (SORN) for this system?	114VA16		
7. Has this SORN been reviewed or updated within the last three years?	Yes three years ago		
Date of Report (MM/YYYY):			15-May-13

Any check mark in the boxes below will require a full PIA. Please continue to the next TAB and complete the remaining		
If there is no Personally Identifiable Information on your system, please complete TAB 2 & TAB 12. (See Comment for Definition		
<input type="checkbox"/> Have any changes been made to the system since the		
<input type="checkbox"/> Is this a PIV system/application/program collecting PII data from Federal employees, contractors, or others performing work for the VA?		
<input checked="" type="checkbox"/> Will this system/application/program retrieve information on the basis of name, unique identifier, symbol or other PII data?		
<input checked="" type="checkbox"/> Does this system/application/program collect, store, or disseminate PII/PHI data?		
<input checked="" type="checkbox"/> Does this system/application/program collect, store or disseminate the SSN?		

(FY 2013) PIA: System of Records

1. Is there a SORN (System of Records Notice) already in place?

☒ Yes☐ No

***If Yes, select all of the appropriate SORN number(s) and continue to Tab 4:
***If No, continue to question 2

***Click to add. Delete SORN by highlighting SORN and comma if included and press the Delete key or place focus on area to delete all SORNs.

LIST OF SORN NUMBER(S) :

114VA16

For each applicable System(s) of Records, list:

2. If records are retrieved using any of the following entities, A SORN will be required (Please check all that apply)

<input checked="" type="checkbox"/>	Full Name
<input checked="" type="checkbox"/>	Maiden
<input type="checkbox"/>	Mother's Maiden
<input checked="" type="checkbox"/>	Alias
<input checked="" type="checkbox"/>	Social Security
<input checked="" type="checkbox"/>	Passport Number
<input type="checkbox"/>	Driver's License
<input type="checkbox"/>	Taxpayer Identification
<input type="checkbox"/>	Financial Account
<input type="checkbox"/>	Credit Card
<input checked="" type="checkbox"/>	Street
<input type="checkbox"/>	Email Address
<input type="checkbox"/>	Photographic
<input type="checkbox"/>	Fingerprints
<input type="checkbox"/>	Handwriting
<input type="checkbox"/>	Other Biometric Data
<input type="checkbox"/>	Other (Explain on Tab 8)

3. Based on Question 2, is a SORN required?

☒ Yes☐ No

***If Yes, has the process begun to obtain/acquire a SORN

☒ Yes☐ No

Location where the specific applicable System of Records Notice may be accessed:

http://www.rms.oit.va.gov/SOR_Records.asp

(FY 2013) PIA: Data Collection And Storage

Please fill in each column for the data types selected.

Data Type	Collection Method	What are the subjects told about the intended use of their information?	How is this message conveyed to them?	How is a privacy notice provided?
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	VA File Database	Claims	Provided By Another System	Provided By Another System
Family Relation (spouse, children, parents, grandparents, etc)	VA File Database	Claims	Provided By Another System	Provided By
Service Information	VA File Database	Claims	Provided By Another System	Provided By Another System
Medical Information	VA File Database	Claims	Provided By Another System	Provided By Another System
Criminal Record Information	N/A	N/A	N/A	N/A
Guardian Information	N/A	N/A	N/A	N/A
Education Information	N/A	N/A	N/A	N/A
Benefit Information	VA File Database	Claims	Provided By Another System	Provided By Another System
Other (Explain on Tab 8)				

Data Type	Storage Method	Source (If requested, identify the specific file, entity and/or name of agency)	Is data collection Mandatory or Voluntary?	
Veteran or Primary Subject's Personal Contact Information (name, address, telephone, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (Identify File)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Family Relation (spouse, children, parents, grandparents, etc)	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (Identify File)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Service Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (Identify File)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Medical Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (Identify File)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Criminal Record Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Guardian Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
Education Information	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	

Benefit Information	<input checked="" type="radio"/> Yes <input type="radio"/> No	VA Files/Databases (Identify File)	<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	Automated
Other (Explain on Tab 8)	<input type="radio"/> Yes <input checked="" type="radio"/> No		<input checked="" type="radio"/> Mandatory <input type="radio"/> Voluntary	
			<i>(Please Select Yes/No)</i>	
Proximity and Timing: Is the privacy notice provided at the time of data collection?			<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No	
Purpose: Does the privacy notice describe the principal purpose(s) for which the information will be used?			<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No	
Authority: Does the privacy notice specify the effects of providing information on a voluntary basis?			<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No	
Disclosures: Does the privacy notice specify routine use(s) that may be made of the information?			<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No	

(FY 2013) PIA: Data Sharing		** Any connection external to VA requires an ISA/MOU per VA 6500. This section below must be consistent with your System Security Plan Interconnection Security Agreement section.			
Organization	Name of Agency/Organization	Do they access this system?	Identify the type of Data Sharing	Is PII or PHI Shared?	What is the procedure you reference for the release of information?
Internal Sharing: VA Organization	Office of Information and Technology (OI&T), Congressional Budget Office (CBO), Service Delivery and Engineering (SD&E), Program Oversight and Informatics (POI).	<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No	Other (Explain in Tab 8)	<input checked="" type="radio"/> Yes <input type="radio"/> No	HIPAA Authorization/Waiver
Other Veteran Organization		<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Other Federal Government Agency	Health and Human Service (HHS), Centers for Medical Services (CMS), via CMS contracted Fiscal Intermediary, Trail Blazer Health Enterprises	<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	HIPAA Authorization/Waiver
State Government Agency		<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Local Government Agency		<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
Research Entity		<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No		<input type="radio"/> Yes <input checked="" type="radio"/> No	
<input type="checkbox"/> Other Project/ System (Explain on Tab 8)					
(FY 2013) PIA: Access to Records					
Does the system gather information from another system?		<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No			
Please enter the name of the system:		VistA, Fee Basis Claims Software (FBCS), Corporate Data warehouse (CDW), Compensation, Pension, Education System (CP&E)			
(FY 2013) PIA: Secondary Use					
Will PII data be included with any secondary use request?		<input checked="" type="radio"/> Yes <input checked="" type="radio"/> No	<input type="checkbox"/> Mental Health	<input type="checkbox"/> HIV	<input type="checkbox"/> Drug/Alcohol Counseling
Check all that apply			<input type="checkbox"/> Sickle Cell	<input type="checkbox"/> Other (Explain on Tab 8)	<input type="checkbox"/> Research

(FY 2013) PIA: Retention & Disposal

What is the data retention period?

Answer: The retention period is seven (7) years for each electronic transmission. This will be based on policy and regulation. Data related to PHI is 75 years from death or date of last access, whichever is longer. Transaction data is seven years. Audit and archive based on RCF 10-1.

Explain why the information is needed for the indicated retention period?

Answer: This will be based on policy and regulation. The agencies retain information in support of issues, references, and/or legal purposes.

What are the procedures for eliminating data at the end of the retention period?

Answer: Data is not eliminated, it is controlled in accordance with National Archives and Records Administration (NARA) control schedules determined by agency.

Where are these procedures documented?

Answer: VA HBK 6300.1 Records Management Procedures explains the Records Control Schedule procedures.

How are data retention procedures enforced?

Answer: VA Directive 6300 , Records and Information Management contains the policies and responsibilities for VA 's Records and Information Management program. VA Handbook 6300.1. Records Management Procedures, contains mandatory procedures for the proper management of records effectively and efficiently throughout their life cycle. Neither the directive or handbook is a Records Control Schedule. Procedures are enforced by Records Management Staff and VA Records Officers.

Has the retention schedule been approved by the National Archives and Records Administration (NARA)

☐ Yes ☒ No (Explain on Tab

(FY 2013) PIA: Children's Online Privacy Protection Act (COPPA)

Will information be collected through the internet from children under age 13?

☐ Yes (Explain on Tab 8) ☒ No

(FY 2013) PIA: Security

Based upon NIST 800-60, volume II; List the Information data types chosen as a basis for your FIPS 199 System Categorization.

Answer:	D14-Health	
Is the system/application/program following IT security Requirements and procedures required by federal law and policy to ensure that information is appropriately secured.	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Has the system/application/program conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls.	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security monitoring conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is security assessment conducted annually or as needed to ensure that controls continue to work properly, safeguarding the information?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
Is adequate physical security in place to protect against unauthorized access?	<input checked="" type="radio"/> Yes	<input type="radio"/> No (Explain on Tab 8)
*Ensure PE 2, PE-3, PE-6, PE-7, PE-8 have been addressed appropriately for your categorization		

Explain what security risks were identified in the security assessment? (Check all that apply)

<input checked="" type="checkbox"/> Biological	<input checked="" type="checkbox"/> Fire	<input checked="" type="checkbox"/> Lightning Strike	<input type="checkbox"/> Terrorist
<input type="checkbox"/> Blizzard	<input checked="" type="checkbox"/> Flood	<input checked="" type="checkbox"/> Malicious Code	<input checked="" type="checkbox"/> Thunderstorm
<input type="checkbox"/> Burglary/Break	<input checked="" type="checkbox"/> Hacker, Cracker	<input checked="" type="checkbox"/> Password Privacy Negligence	<input checked="" type="checkbox"/> Tornado
<input type="checkbox"/> Civil Unrest	<input checked="" type="checkbox"/> Hail	<input type="checkbox"/> Personnel Unavailable	<input type="checkbox"/> Tsunami
<input checked="" type="checkbox"/> Component	<input type="checkbox"/> HAZMAT Release/Spill	<input checked="" type="checkbox"/> Power Failure	<input checked="" type="checkbox"/> User Negligence
<input type="checkbox"/> Dam Failure	<input type="checkbox"/> Human Health Emergency	<input type="checkbox"/> Sabotage	<input checked="" type="checkbox"/> User Sabotage
<input type="checkbox"/> Dust/Debris	<input checked="" type="checkbox"/> Hurricane	<input checked="" type="checkbox"/> System Intrusion, Break-Ins	<input type="checkbox"/> Vibration
<input checked="" type="checkbox"/> Earthquake	<input checked="" type="checkbox"/> HVAC Failure	<input checked="" type="checkbox"/> System Misconfiguration	<input type="checkbox"/> Volcano
<input checked="" type="checkbox"/> Extreme Cold	<input type="checkbox"/> Indoor Humidity	<input checked="" type="checkbox"/> System Penetration	<input checked="" type="checkbox"/> Water Damage
<input type="checkbox"/> Extreme Heat	<input type="checkbox"/> Landslide	<input type="checkbox"/> System Tampering	<input type="checkbox"/> Winter Weather Hazards

*If any other risks identified, explain in Tab 8

Based upon the risks identified above, explain what security controls are being used to mitigate these risks. (Check all that apply)

<input checked="" type="checkbox"/> Access Control	<input checked="" type="checkbox"/> Configuration Management	<input checked="" type="checkbox"/> Media Protection	<input checked="" type="checkbox"/> System and Services Acquisition
<input checked="" type="checkbox"/> Audit and	<input checked="" type="checkbox"/> Contingency Planning	<input checked="" type="checkbox"/> Personnel Security	<input checked="" type="checkbox"/> System and Communication Protection
<input checked="" type="checkbox"/> Awareness and	<input checked="" type="checkbox"/> Identification and Authentication	<input checked="" type="checkbox"/> Physical and Environmental Protection	<input checked="" type="checkbox"/> System and Information Integrity
<input checked="" type="checkbox"/> Security Assessment and Authorization	<input checked="" type="checkbox"/> Incident Response	<input checked="" type="checkbox"/> Risk Assessment	<input checked="" type="checkbox"/> Planning <input checked="" type="checkbox"/> Maintenance

Answer: (Other Controls) Explain on Tab 8

PIA: PIA Assessment

The PIA assessment is based on FIPS 199 which can be found within your system security plan (SSP).

<u>Availability Assessment:</u> If the data being collected is not available to process for any reason what will the potential impact be upon the system or organization? (Choose One)	<input type="radio"/> The potential impact is high if the loss of availability could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	<input type="radio"/> The potential impact is moderate if the loss of availability could be expected to have a serious adverse effect on operations, assets or individuals.
	<input checked="" type="radio"/> The potential impact is low if the loss of availability could be expected to have a limited adverse effect on operations, assets or individuals.
<u>Integrity Assessment:</u> If the data being collected has been corrupted for any reason what will the potential impact be upon the system or organization? (Choose One)	<input type="radio"/> The potential impact is high if the loss of integrity could be expected to have a severe or catastrophic adverse effect on operations, assets or individuals.
	<input type="radio"/> The potential impact is moderate if the loss of integrity could be expected to have a serious adverse effect on operations, assets or individuals.
	<input checked="" type="radio"/> The potential impact is low if the loss of integrity could be expected to have a limited adverse effect on operations, assets or individuals.
<u>Confidentiality Assessment:</u> If the data being collected has been shared with unauthorized individuals what will the potential impact be upon the system or organization? (Choose One)	<input checked="" type="radio"/> The potential impact is high if the loss of confidentiality could have a severe or catastrophic adverse effect on operations, assets or individuals.
	<input type="radio"/> The potential impact is moderate if the loss of confidentiality could be expected to have a serious adverse effect on operations, assets or individuals.
	<input type="radio"/> The potential impact is low if the loss of confidentiality could be expected to have a limited adverse effect on operations, assets or individuals.

The controls are being considered for the project based on the selections from the previous assessments?

The minimum security requirements for our high impact system cover seventeen security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

(FY 2013) PIA: Additional Comments

Add any additional comments or information that may have been left out for any question. Please indicate the question you are responding to and then add your comments.

Tab 4 lines 28-44 files and databases:

Internal Sharing: VA Organization The application will interface to VA Purchase Care databases, feeding a repository with a claims scoring tool that will score incoming claims for risk of fraud, waste and abuse.

PCI gathers information from the following systems. VistA, Fee Basis Claims Software (FBCS), Corporate Data warehouse (CDW), Compensation, Pension, Education System (CP&E)

Tab 5 Row 4, Column D

PCI is deployed at AITC to store data fetched from multiple VA internal sites. The PCI reporting engine server allows business users from multiple locations within VA environment. The PCI scoring tool allows all claim processing systems deployed at sites to interact with the scoring tool, the reporting tool and the predictive analytics tool to access data. These VA internal agencies access PCI claim data information: Office of Information and Technology (OI&T), Congressional Budget Office (CBO), Service Delivery and Engineering (SD&E).

(FY 2013) PIA: VBA Minor Applications

Which of these are sub-components of your system?

Access Manager	Automated Sales Reporting (ASR)	Automated Folder Processing System (AFPS)
Actuarial	BCMA Contingency Machines	Automated Medical Information Exchange II (AIME II)
Agent Orange	Centralized Property Tracking System	Automated Medical Information System (AMIS)290
Appraisal System	Common Security User Manager (CSUM)	Automated Standardized Performance Elements Nationwide (ASPEN)
ASSISTS	Compensation and Pension (C&P)	Centralized Accounts Receivable System (CARS)
Awards	Control of Veterans Records (COVERS)	Committee on Waivers and Compromises (COWC)
Baker System	Courseware Delivery System (CDS)	Compensation and Pension (C&P) Record Interchange (CAPRI)
Bbraun (CP Hemo)	Dental Records Manager	Compensation & Pension Training Website
Broome Closet	Education Training Website	Distribution of Operational Resources (DOOR)
C&P Payment System	Electronic Appraisal System	Educational Assistance for Members of the Selected Reserve Program CH 1606
C&P Training Website	Electronic Card System (ECS)	Electronic Performance Support System (EPSS)
CONDO PUD Builder	Electronic Payroll Deduction (EPD)	Enterprise Wireless Messaging System (Blackberry)
EndoSoft	Eligibility Verification Report (EVR)	Financial Management Information System (FMI)
FOCAS	Fiduciary Beneficiary System (FBS)	Hearing Officer Letters and Reports System (HOLAR)
Inforce	Fiduciary STAR Case Review	Inquiry Routing Information System (IRIS)
INS - BIRLS	Financial and Accounting System (FAS)	Modern Awards Process Development (MAP-D)
Insurance Online	Insurance Unclaimed Liabilities	Personal Computer Generated Letters (PCGL)
Insurance Self Service	Inventory Management System (IMS)	Personnel Information Exchange System (PIES)
LGY Home Loans	Interactive Voce Response (IVR)	Post Vietnam Era educational Program (VEAP) CH 32
LGY Processing	LGY Centralized Fax System	Purchase Order Management System (POMS)
MES	Loan Service and Claims	Reinstatement Entitlement Program for Survivors (REAPS)
Mobilization	Loan Guaranty Training Website	Reserve Educational Assistance Program CH 1607
Montgomery GI Bill	Mental Health Assistant	Service Member Records Tracking System
MUSE	National Silent Monitoring (NSM)	Survivors and Dependents Education Assistance CH 35
Omnicell	Powerscribe Dictation System	Systematic Technical Accuracy Review (STAR)
Priv Plus	Rating Board Automation 2000 (RBA2000)	Training and Performance Support System (TPSS)
RAI/MDS	Records Locator System	VA Online Certification of Enrollment (VA-ONCE)
RightFax	Remittance Processing System	VA Reserve Educational Assistance Program
Right Now Web	Review of Quality (ROQ)	Veterans Assistance Discharge System (VADS)
SAHSHA	Search Participant Profile (SPP)	Veterans Exam Request Info System (VERIS)
Script Pro	Spinal Bifida Program Ch 18	Veterans Insurance Claims Tracking and Response System (VICTARS)
SHARE	State Benefits Reference System	Veterans Service Representative (VSR) Advisor
Sidexis	State of Case/Supplemental (SOC/SSOC)	Vocational Rehabilitation & Employment (VR&E) CH 31
Synquest	Telecare Record Manager	Web Automated Folder Processing System (WAFPS)
VBA Training Academy	VBA Enterprise Messaging System	Web Automated Reference Material System (WARMS)
Veterans Canteen Web	Web Electronic Lender Identification	Web Automated Verification of Enrollment
VETSNET Housekeeping		Web-Enabled Approval Management System (WEAMS)
VR&E Training Website		Web Service Medical Records (WebSMR)
Web LGY		Work Study Management System (WSMS)

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name	
Description	
Comments	
Is PII collected by this min or application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

Name	
Description	
Comments	
Is PII collected by this min or application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

(FY 2013) PIA: VHA/NCA Minor Applications A-M

Which of these are sub-components of your system?

1184 Web	Clinical Data Repository/Health Data Repository	IFCAP
A4P	Clinical Info Resource Network	Imaging
ACCU Care	Clinical Monitoring System	Incentive Awards
ACCU Check	Clinical Notes Templates	INCORE 2
ACCU Med	Clinical Procedures	ENDSOFT
Adobe Acrobat	Clinical Reminders	Engineering
ADP Planning (PlanMan)	Clippership	Enrollment Application System
ADT	Combat Veteran Outreach	Enterprise Terminology Server & VHA Enterprise Terminology Services
Adverse Reaction Tracking	Committee on Waiver and Compromises	Integrated Billing
Agent Cashier	Consult/ Request Tracking	ePROMISE
Air Fortress	Controlled Correspondence	Equipment/ Turn-in Request
ASISTS	Controlled Substances	Event Capture
Authorization/ Subscription	CP&E	Event Driven Reporting
Auto Instrument	CPRS	Extensible Editor
Auto Replenishment/ Ward Stock		External Peer Review
AUTOCAD	CPT/ HCPCS Codes	EYECAP
Automated Access Request	Credentials Tracking	Fee Based Claims System
Automated Info Collection Sys	Credit Card Authentication	Fee Basis
Automated Lab Instruments	Data Innovations	Financial and Accounting System (FAS)
Automated Med Info Exchange	DELIVEREX	Financial Management System (FMS)
Automated Sales Reporting	Dental	Functional Independence
AutoMed	DICTATION-Power Scribe	Gen. Med. Rec. - I/O
Bad Code Med Admin	Dietetics	Gen. Med. Rec. - Vitals
Barcode Medication Administration Contingency Plan (BCU)		Gen. Med.Rec. - Generator
BCMA Contingency Workstations		GENDEX
BDN 301	Discharge Summary	Generic Code Sheet
Beneficiary Travel	DRG Grouper	Genesys
Big Fix	DRM Plus	Get Well Networks
BHL	Drug Accountability	GMED
CA Vertified Components - DSSI	DSIT	GRECC
Capacity Management - RUM	DSS Extracts	Health Data and Informatics
Capacity Management Tools	DSS Quadramed	Health Level Seven
CAPRI	EDS Whiteboard (AVJED)	Health Summary
Cardiff Teleform	Education Tracking	Health Summary Contingency
Cardiology Systems (stand alone servers from the network)		HINQ
Care Management	EEO Complaint Tracking	Hospital Based Home Care
CareTracker	EKG System	ICB
CHECKPOINT	Electronic Card System (ECD)	
Citrix	Electronic Payroll Deduction (EPD)	
Clinical Case Registries	Electronic Signature	ICR - Immunology Case Registry

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

Name	
Description	
Comments	
Is PII collected by this minor application?	
Does this minor application store PII?	
If yes, where?	
Who has access to this data?	

(FY 2013) PIA: VHA/NCA Minor Applications N-Z

Which of these are sub-components of your system?

National Cemetery Association	Pharmacy Prescription Practice	Scheduling	VAMedSafe
National Drug File	PICIS OR	Security Suite Utility Pack	VBECs
National Laboratory Test	Police & Security	Sentillion	VDEF
NDBI	Problem List	Shift Change Handoff Tool	Vendor - Document Storage Sys
Network Health Exchange	Progress Notes	ShoreTel	Veterans Canteen Web
NOAHLINK	Prosthetics	Social Work	Veterans Information Solution
NOIS	Purchase Order Management System		VHAHUNAPP1
Nursing Service	Pyxis	Stellant	VHAHUNFPC1
Occurrence Screen	Q-Matic	Stentor	VHS & RA Tracking System
Omnicell	QMSI Prescription Processing	Surgery	Visit Tracking
Oncology	Quality Assurance Integration	Survey Generator	VISTA RAD
Onvicord (VLOG)	Quality Improvement Checklist	Telecare Record Manager	VISTA RO
Optifill	QUASER	Temp Trak	VistALink
Order Entry/ Results Reporting	Radiology/ Nuclear Medicine	Text Integration Utilities	VistALink Security
Outpatient Pharmacy	RAFT	Tickler Database	Visual Impairment Service Team ANRV
P2000 ROBOT	RALS	Toolkit	
PACS database	Record Tracking	TopCon	Vitria BusinessWare
Patch Module	Registration	TraceMaster	VIXS
Patient Data Exchange	Release of Information - DSSI	Tracking Continuing Education	
Patient Feedback	Remote Order/ Entry System	Traumatic Brain Injury	Voluntary Timekeeping
Patient Representative	RPC Broker	Unwinder	Voluntary Timekeeping National
PCE Patient Care Encounter	Run Time Library	Utility Management Rollup	WEB HINQ
Personal Computer Generated Letters		Utilization Review	Whiteboard
Pharmacy Benefits Mangement	SAGG	VA Conference Room Registration	
Pharmacy Data Management	SAN	VA Fileman	Women's Health
Pharmacy National Database	Scanning Exam and Evaluation System		Workload and Overtime

Explain any minor application that are associated with your installation that does not appear in the list above. Please provide name, brief description, and any comments you may wish to include.

Name			
Description			
Comments			
Is PII collected by this minor application?			
Does this minor application store PII?			
If yes, where?			
Who has access to this data?			

Name			
Description			
Comments			
Is PII collected by this minor application?			
Does this minor application store PII?			
If yes, where?			
Who has access to this data?			

Name			
Description			
Comments			
Is PII collected by this minor application?			
Does this minor application store PII?			
If yes, where?			
Who has access to this data?			

(FY 2013) PIA: Final Signatures			
Facility Name:	Austin Information Technology Center (AIRC)		
Title:	Name:	Phone:	Email:
Privacy Officer:	Amy Howe	512-326-6217	amy.howe1@va.gov
Digital Signature Block			
Information Security Officer:	Juan Rivera	732-578-5495	juan.rivera5@va.gov
Digital Signature Block			
System Owner/Delegate:	Tammy Watson	202-461-6126	tammy.watson@va.gov
Digital Signature Block			
Facility Chief Information Officer	N/A	N/A	N/A
Digital Signature Block			
Information Owner:	0	0	0
Digital Signature Block			
Other Titles:	0	0	0
Digital Signature Block			
Date of Report:	15-May-13		
OMB Unique Project Identifier	029-00-01-11-01-5108-00		
Project Name	CDCO > AIRC > VA > Purchase Care Program Integrity Tool		